Notice of Allowability	Application No.	Applicant(s)	
	10/049,258	SCHWENK, JOERG	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 5/22/06.

2. ☒ The allowed claim(s) is/are 9-16.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 1/28/02
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

1. Claims 9-16 are pending.

2. The response of 5/22/06 has been received and entered.

Reasons for Allowance

Claim 9 recites:

Matayas, US patent 5201000 discloses a method for at least one of generating and regenerating an encryption key for a cryptographic method, comprising:

- Generating a seed S, the seed S being a large random number, only on a side of a user by consulting at least one quantity u known only to the user, the encryption key C and a public key U being generated from the seed S by using at least one predefined deterministic method, where the seed S is the information used to generate the key and the quantity u is the passphrase, and C is the private key PRi and U is the public key PUi. (Figure 13) & Abstract & (column 4, lines 54 – column 5, lines 60)
- Storing a regeneration information R so that the regeneration information R is secured against loss, where R is used to regenerate the key. (Figure 13) & Abstract & (column 4, lines 54 – column 5, lines 60)
- Wherein if the encryption key C is unavailable then the key C is reconstructable by the trust center by linking the regeneration information to the seed. (Figure 13) & Abstract & (column 4, lines 54 – column 5, lines 60)

Matayas fails to disclose:

- Generating a regeneration information R on the side of the user to regenerate the seed S and from which the seed S may be derived deterministically by a trust center by linking only to a secret information v known to the trust center;
- Storing the regeneration information R so that the regeneration information R is secured against loss
- Wherein if the encryption key C is unavailable then the seed S is reconstructable by the trust center by linking the regeneration information to the secret information v.

Leighton US patent 5647000 further discloses a method where a trust center stores a seed (figure 1) which may be used to regenerate a key.

However neither Matayas or Leighton disclose an embodiment wherein a regeneration information is used to regenerate a seed. Typically in the prior art, a seed or variant (hashed or encrypted) thereof is used to regenerate a key. To seek to store information to regenerate a seed is atypical. A seed is understood in the art to be a piece of information from which a key is derived and often takes the form of a large random number. A search of the prior art of record has not uncovered the step of generating or storing a regeneration information on the side of the user from which the seed S may be derived

deterministically by a trust center by linking only to a secret information v known to a trust center.

However SSL or secure sockets layer is a protocol well known to those of ordinary skill in the art. SSL derives its keys using a master secret which is used to derive keys. The master secret is derived from a "pre-master secret" which is generated by the client which means it is necessarily stored on the client side for at least a temporary period of time. This pre-master secret may be used to regenerate a seed S, the master secret, which is then used in turn to derive keys. Information on this process can be found in the SSL 3.0 specification which was created in 1996.

However, no art of record can be found where the seed is may be derived deterministically by linking to a secret information known v only to a trust center. In particular, the pre-master secret of SSL can not be derived from a trust center because it is generated on the client side through a pseudorandom function. Furthermore, the pre-master secret in SSL is discarded after its usage.

For this reason, claim 9 distinguishes over the prior art and is allowable.

Claims 10-16 are dependent on claim 9 and are allowable because claim 9 is allowable.

Conclusion

3. The following art not relied upon is made of record:

- Us patent 6345098 discloses a method for improved reliability in generating cryptographic variables
- US patent 6148404 discloses a method where authentication data is generated using a seed and secret key and a second seed data is stored.
- US patent 5321749 discloses an encryption device where a password from a user is used as a seed for a random number generating towards generating cryptographic information
- "SSL 3.0 specification" Netscape Communications, November 18th 1996.

4. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799.**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

August 6th, 2006

KAMBIZ ZAND
PRIMARY EXAMINER